UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated, Plaintiff, v. ALLY BANK and ALLY FINANCIAL INC., Defendants.	Civil Action No.: 21-cv-6799-NSR

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS AMENDED COMPLAINT

KANTROWITZ GOLDHAMER & GRAIFMAN. P.C.
16 Squadron Blvd., Suite 106
New City, NY 1056
T: (845) 356-2570

[*Additional Attorneys on Signature Page*]

Attorneys for the Plaintiff and Members of the Putative Class

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Rules

Other Authorities

Plaintiff David De Medicis (the "Plaintiff"), by and through his undersigned counsel, respectfully submits this Memorandum of Law in Opposition of Defendants' Motion to Dismiss the Amended Complaint, Dkt. 45, filed January 9, 2023 (the "AC").

Preliminary Statement

Beginning on or before February 18, 2021, and continuing until April 12, 2021, without Plaintiff's or putative Class member's knowledge or authority, the confidential usernames and passwords Plaintiff's and putative Class members use to open, maintain and transact in their Ally Bank were disseminated in clear unencrypted text to strangers unknown to Plaintiff and Class members when they logged into Ally Bank accounts via Ally.com, a website operated by defendants Ally Bank and Ally Financial Inc. (collectively "Ally"). Unauthorized recipients forwarded those Sign-in Credentials to additional unauthorized recipients without the Plaintiff's or Class member's knowledge or authority, and so on (the "Breach").

As a result, unauthorized third parties possessed Plaintiff's and Class member's compromised Sign-in Credentials for a period spanning at least three months without Ally even being aware of the Breach. Sign-in Credentials are the confidential "keys" used by Ally Bank customers to maintain the security of cash, credit and other assets as well as the Private Information (as defined) associated with maintaining and transacting in Ally Bank accounts. Maintaining confidentiality of Sign-in Credentials is imperative to online security as acknowledged by defendants.

Ally claims it acted immediately after learning of the Breach, to require that usernames and passwords be changed. But crucial to this motion, Ally does not address the months long opportunity for the compromised Sign-in Credentials to be exploited by wrongdoers before they were changed.

Ally also claims that it requested unauthorized recipients return the Sign-in Credentials to Ally. Ally's need to ask for return of the compromised Sign-in Credentials suggests that the Sign-in Credentials were not safe or secure from possession by unauthorized third parties. Further, Ally cannot and did not address the extent to which the compromised Sign-in Credentials were further distributed by the unauthorized third parties who had possession of it for months prior to Ally's asking for it back.

Plaintiff and the Class were injured and in addition are exposed to significant risk of future injury. Several of the Plaintiff's online accounts have been targeted by malicious actors as set forth herein. In addition, in just a few days during August 2022, hackers engaged in a coordinated attack upon many thousands of Ally Bank customers in what can reasonably be inferred to as use of a subset of information compromised from the Breach. For example, as detailed in the AC, Ally customers complained of unauthorized transactions with Ally Bank accounts that had never been used before. This sort of information would have been accessible to hackers using breached Sign-in Credentials. Ally customers posted that the August 2022 mass attack seems linked to the Ally Breach announced in June 2021.

In August 2022, in response to substantial public discourse about the wave of fraud impacting Ally customers, Ally was forced to acknowledge that because of the increase in attacks Ally's call center wait time was longer than normal.

The Amended Complaint adequately pleads facts demonstrating Plaintiff's Article III standing under both present injury and substantial likelihood of future injury. Notably, Ally does not disclose how the Coding Error manifested, that is, whether or not the Coding Error itself was the product of a malicious hacker. Whether the so-called Coding Error was Ally's own doing is a question of fact.

Regardless, under *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021). Plaintiff pleads facts that demonstrate Article III standing even if the Coding Error was Ally's own doing (i) the exposure was unintentional; (ii) exposed information was misused; and (iii) exposed information was sensitive and high risk.

The Plaintiff pleads a plausible nexus between the Breach and the injuries. Information needed to hack Plaintiff's online accounts was the same sort of information compromised in the Breach. Further, online postings from customers who are not parties in this action but were bank customers subject to intrusion of their accounts, understood the nexus between the Breach and the subsequent wave of organized attacks on Ally Bank accounts in August 2022.

Finally, in addition to Article III standing and injury, Plaintiff alleges sufficient facts for each of his claims of negligence, negligence per se, breach of implied contract, North Carolina Unfair & Deceptive Trade Practices Act, Virginia Personal Information Breach Notification Act, and declaratory/injunctive relief to withstand a motion to dismiss under Rule 12(b)(6).

The Amended Complaint must be sustained.

Factual Background

A. Ally's Data Breach

For months Ally recklessly or negligently failed to take reasonable steps to test or monitor the security of Ally.com, a website used by Plaintiff and Class members to open, maintain, review and transact in their accounts at Ally Bank.

At all times Ally knew that maintaining the security and confidentiality of Sign-in Credentials was a critical banking service to Plaintiff and the Class. Acknowledging that duty Ally stated "[W]e never share your usernames and passwords with anyone . . ." Ally knew that, if Sign-in Credentials were compromised, Plaintiff and the Class would be exposed to imminent risk

of injury because compromised bank sign-in credentials are frequently sold on black markets to identity thieves and fraudsters.

In addition to the Sign-in Credentials themselves, Plaintiff's Ally Bank Sign-in Credentials were linked and provided access to an array of other personal, confidential data entrusted to Ally, which was associated with opening and transacting in Ally Bank accounts, including (a) full names and physical addresses; (b) email addresses; (c) account numbers; (d) current account balances; (e) checking account statements; (f) savings account statements; (g) investment account statements; (h) images of all cancelled checks; (i) names of account beneficiaries; (j) birth dates of account beneficiaries; (k) employment information; (l) the names of bank accounts linked to Ally Bank accounts; (m) last four digits of account numbers of bank accounts linked to Ally Bank accounts; (n) IRS tax forms; (o) last four digits of Social Security numbers; (p) Zelle account information; (q) and Zelle transaction history ("Private Information"). Compromising Private Information exposed Plaintiff and Class members to identity theft in numerous ways.

Nonetheless, beginning on or before February 18, 2021 and continuing until April 12, 2021, when Plaintiff and Class members logged into accounts at Ally Bank via the Ally.com customer portal, without permission or knowledge, Ally disseminated their Sign-in Credentials in clear unencrypted text to unauthorized third parties unknown to Plaintiff or Class members.

Whether the malfunction that caused unauthorized dissemination of Sign-in Credentials was prompted by malicious conduct or Ally's own recklessness has not been publicly revealed by Ally. Either scenario is plausible. Ally has provided no explanation about how or why the malfunction that improperly disseminated Sign-in Credentials which Ally refers to as an unintended Coding Error manifestation.

Regardless, had Ally properly monitored the operation and security of Ally.com during the months of February through April 2021, the Breach could have been avoided entirely. But Ally did not. Indeed, Ally claims to have first become aware of the website malfunction on April 12, 2021 during a routine website update.[1] Repair of the malfunctioning website was accomplished the very same day it was purportedly discovered.

Ally does not address the fact that Sign-in Credentials were in possession of unauthorized third parties for months without Ally's knowledge. It is alleged that the unauthorized third parties disseminated the Sign-in Credentials to additional unauthorized persons. The full extent of dissemination of data compromised in the Breach is not known. Use of the types of data compromised in the Breach creates a plausible inference that at least a subset of data was used to commit identity theft.

B. Ally's Unreasonable Delay in Disclosing its Breach

As of April 12, 2021, Ally knew of the Breach and knew that security of Sign-in Credentials had been compromised for months. Ally should have immediately notified Plaintiff and other Class members that accessing Ally Bank accounts via Ally.com during February through April 2021 risked of unauthorized dissemination of their Sign-in Credentials and compromised the security of all Personal Information associated with their Ally Bank accounts. But Ally did not.

Ally instead unreasonably delayed disclosing the Breach for its own benefit to devise a strategy to minimize its wrongful conduct and oversight failures. Ally put off any disclosure of the Breach for an additional two months until June 11, 2021. When Ally finally did disclose the Breach it did so in a way that misleadingly minimized its wrongdoing. Ally's belated public

[1] Notably, the Hall declaration speaks only to events occurring after Ally's malfunctioning website was repaired and not to Ally's improper conduct during February 18, 2021 until April 12, 2021, such as Ally's failure to properly test or monitor the security of the website.

disclosure of the Breach omitted that its website had improperly disseminated Sign-in Credentials in clear unencrypted text completely unnoticed by Ally's security systems for a period spanning three months! Why so long? Ally also omitted how the coding error manifested including whether the unintended Coding Error was malicious. The Breach notification creates a misleading impression that the Coding Error almost immediately had been corrected rather than the actual fact — e.g., that it persisted for months.

C. The Ally Breach has caused injury

Plaintiff and the Class were subjected to fraudsters apparently using compromised information in the wake of the Breach to hack their online accounts and engage in identity theft. For example, in April 2021 fraudsters used an Ally Bank account to make unauthorized transactions at a Home Depot store the customers had never visited; in May 2021 a customer reported that $3,000 in securities were taken from his Ally account; in August 2021, an Ally customer reported incurring late charges because several bill payments from his Ally debit account were declined following a fraud alert; in October 2021 a customer was notified by Ally that the email associated with his Ally account was changed without his knowledge and was unable to pay bills with his Ally account.

D. Plaintiff Injuries caused by Ally's Breach

Similarly, fraudsters hacked Plaintiff's accounts resulting in the Plaintiff being prohibited from accessing the assets in his accounts and fraudsters using Plaintiff's accounts to conduct unauthorized transactions.

- From August 18, 2021 until August 27, 2021, Ally froze the Plaintiff's Ally Bank accounts and prohibited Plaintiff from accessing his funds on deposit in those accounts to purchase securities at favorable market prices.
- On September 11, 2021, Ally alerted Plaintiff of an unauthorized attempt to break into Plaintiff's Ally Bank accounts.

- On September 11, 2021, hackers purportedly from Russia and the Netherlands began repeated attempts to sign in, gain access to, and take over Plaintiff's personal email account.
- On November 16, 2021, the FanDuel notified the Plaintiff of multiple malicious attempts to break into his FanDuel account.
- On October 21, 2022, a malicious actor broke into Plaintiff's Coinbase account and engaged in several authorized transactions including an attempt to transfer funds from Ally Bank to Coinbase.
- Since October 2022, Ally has frozen Plaintiff Ally Bank accounts on at least twice because of suspicious activity.
- On October 27, 2022, Plaintiff's Ally Bank accounts were hacked which required closing and reopening those accounts with different account numbers.
- On October 28, 2022, a fraudster hacked Plaintiff's Amazon account and making two unauthorized purchases using Plaintiff's PNC Bank credit card.

E. Misuse of data compromised data in the Breach

Beginning in August 2022, the actual effects of the Ally Breach manifested in certain customer's accounts and a wave of thousands of Ally Bank debit and credit card accounts were subjected to unauthorized transactions as part of an apparent organized attack raising a plausible inference that at least a portion of the data compromised in the Ally Breach was used by malicious actors. The fraud is reflected in a "giant spike" in fraud related communications by Ally customers on Reddit.com.

F. Ally acknowledges an increase in fraudulent activity

An Ally spokesperson acknowledged the increase in fraudulent activity caused by bad actors and that Ally's call centers were experiencing longer than usual wait times.

G. Risk of Future Injury

As reflected in the wave of fraudulent activity beginning in August 2022 and ongoing targeting of the Plaintiff's online accounts. The fact that misuse of compromised data occurs years after a breach is well recognized. This case is a clear example of that timeline.

H. The Court's Order regarding the original Complaint

The Court dismissed the original complaint pursuant to FRCP 12(b)(1) on August 2, 2022 "without prejudice" holding the Complaint failed to establish the injury requirement for Article III standing. ECF No. 29 at 8-16 ("Opinion"). The Court stated that factual assertions in Plaintiff's affidavit could not be considered as encompassed in that pleading (Opinion at 15).

I. The Amended Complaint cures all Deficiencies

The Amended Complaint alleges far more hacking of Plaintiff's accounts than pled in the original complaint or Plaintiff's affidavit. The Amended Complaint also pleads a coordinated attack that occurred in August of 2022 on many thousands of Ally customers through apparent use of the types of Private Information compromised in the Ally Breach. The Amended Complaint does not allege the so-called Coding Error was Ally's own doing. It is plausible that the Coding Error was the result of malicious conduct on the part of a third party and based on the pleading herein, and the reasonable inferences to be afforded it, there is no basis to assume the Breach arose merely from Ally's own negligence and was not contributed to by an outside actor.

Substantial risk of ongoing future harm exists here. Thousands of Ally accounts have already been targeted by fraudsters. AC ¶¶ 98-107. Facts in the AC adequately reflect that an unauthorized third party purposefully obtained the Plaintiff's and class members' private data; at least a portion of compromised data has been misused; and that the highly sensitive types of data compromised create a high risk of ongoing identity theft against the Plaintiff and class members.

In sum, all of the deficiencies in the original complaint identified by the Court have been cured. The Amended Complaint states plausible grounds for relief and should be sustained.

ARGUMENT

II. THE AMENDED COMPLAINT ALLEGES ARTICLE III STANDING

A. Legal Standard

The " 'irreducible constitutional minimum" of standing consists of three elements': the individual initiating the suit 'must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.' " *Dhinsa v. Krueger*, 917 F.3d 70, 77 (2d Cir. 2019) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 136 S. Ct. 1540, 1547, 194 L.Ed.2d 635 (2016)).

Challenges to Article III standing are addressed under Federal Rule of Civil Procedure 12(b)(1), which governs motions to dismiss for lack of subject matter jurisdiction. *In re Blackbaud, Inc., Customer Data Breach Litig*., 3:20-MN-02972-JMC, 2021 WL 2718439, at *4 (D.S.C. July 1, 2021) ("*In re Blackbaud*"); *See also*, *CGM, LLC v. BellSouth Telecomms., Inc.*, 664 F.3d 46, 52 (4th Cir. 2011).

1. On a Factual Attack the Court Employs a Summary Judgment Standard And if the Jurisdictional and Merits Facts are Intertwined, Discovery Should Proceed

A defendant may contest subject matter jurisdiction under Rule 12(b)(1) through a facial attack or a factual attack. *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009). In a facial attack, the defendant contends "that a complaint simply fails to allege facts upon which subject matter jurisdiction can be based." *Kerns, supra,* at 192 (quoting *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). In a factual challenge, the defendant asserts "'that the jurisdictional allegations of the complaint [are] not true.'" *Id.* (quoting *Adams*, 697 F.2d at 1219). Thus, a trial court may "go beyond the allegations of the complaint" and "consider evidence by affidavit, depositions or live testimony without converting the proceeding to one for summary judgment." *Adams*, 697 F.2d at 1219; *In re Blackbaud* at *4.

But if the jurisdictional facts "are so intertwined with the facts upon which the ultimate issues on the merits must be resolved," the "entire factual dispute is appropriately resolved only by a proceeding on the merits." *U.S. ex rel. Vuyyuru v. Jadhav*, 555 F.3d at 348 (citing *Adams*, 697 F.2d at 1219-20); *In re Blackbaud*, at *4-5:

When a defendant makes a factual attack to subject matter jurisdiction and the jurisdictional and merits facts are intertwined,

> the trial court should assume jurisdiction exists (if the jurisdictional allegations are sufficient on their face) and proceed with limited or full discovery after either (1) denying the 12(b)(1) motion, or (2) converting the 12(b)(1) motion into a motion for summary judgment on the merits and taking it under advisement until discovery is completed and it is ripe for summary judgment[.]

In re Blackbaud, at *5 (internal citations omitted).

Here, the losses from the Breach include intrusion into the Coinbase Account and Amazon Account, which were linked to Plaintiff's Ally Bank account and Plaintiff's inability to use the funds in the account to purchase securities, are part of the merits-based claims here. Because these raise sufficient triable issues of fact as to his damages as well as proximate cause, the Court should decline the invitation to determine jurisdiction and allow discovery.

Moreover, in assessing a factual challenge under Rule 12(b)(1) which implicates the merits, the Court employs the summary judgment standard. *See, First Cap. Asset Mgmt., Inc. v. Brickellbush, Inc.*, 218 F.Supp.2d 369, 378-79 (S.D.N.Y. 2000) (employing the summary judgment standard); *see also, Morrison v. Amway Corp.*, 323 F.3d 920, 925 (11th Cir. 2003) (noting that in such cases the court "must treat [] the motion as a motion for summary judgment under Rule 56 and refrain from deciding disputed factual issues"); *Barrett Computer Servs., Inc. v. PDA, Inc.*, 884 F.2d 214, 219 (5th Cir. 1989) (same).

2. Plaintiff's Requirement to Show "Traceability" is a Lesser Burden Than Proximate Cause

The requirement that a complaint allege an injury "that is fairly traceable to defendant's conduct for purpose of constitutional standing is a lesser burden than the requirement that it show proximate cause*." Rothstein v. UBS AG,* 708 F.3d 82, 92 (2d Cir. 2013); *Toretto v. Donnelley Fin. Solutions, Inc.*, 523 F.Supp.3d 464, 472 (S.D.N.Y. 2021) (discussing the "traceability" standard in the data breach context). The Second Circuit has noted that "particularly at the pleading stage, the 'fairly traceable' standard is not equivalent to a requirement of tort causation' and that 'for purposes of satisfying Article III's causation requirement, we are concerned with something *less than the concept of proximate cause.*" *Rothstein* at 92 (internal citations omitted).

As stated in *Toretto, supra*, at 472:

> At the pleading stage of an action, as here, "the plaintiff's burden ... of alleging that their injury is 'fairly traceable' to the challenged act is relatively modest." *Id.* (internal quotations and citation omitted). "In sum, the test for whether a complaint shows the "fairly traceable" element of Article III standing imposes a standard lower than proximate cause." *Id.* Rather than a showing of proximate cause, "Article III 'requires no more than *de facto* causality.' " *U.S. Dep't of Com. v. New York*, —— U.S. ——, 139 S. Ct. 2551, 2566, 204 L.Ed.2d 978 (2019) (internal citation omitted).

523 F.Supp.3d at 472.

3. Injury

To satisfy the "injury in fact" element in cases involving allegations of "unauthorized exposure of th[e] plaintiff's data," the complaint must establish either a present injury or a future injury due to the alleged exposure. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300–01 (2d Cir. 2021). A future injury may satisfy the "injury in fact" requirement "only if the threatened injury is certainly impending, or if there is a substantial risk that the harm will occur." *Id.*

Contrary to Defendant's interpretation, the term "misuse" does not require *successful* hacking and profiting from the wrongdoer's misuse of the information. This common sense approach is based on the fact that misuse, even without causing current pecuniary loss demonstrates that there is a substantial risk that a harm will occur, thus serving as a proper pleading predicate for demonstrating *future injury* due to the alleged exposure. The attempts documented in the AC serve to confirm that the information is possessed by a wrongdoer, attempting to successfully profit, even if the attempt is unsuccessful. Thus, these attempts demonstrate that a sufficient misuse has occurred to trigger mitigation efforts which are deemed reasonable to prevent a future injury. In *McMorris*, the Court confirmed this, stating, "evidence that plaintiffs' data is already being misused, ***even if that misuse has not yet resulted in an actual or attempted identity theft,*** can also support a finding that those plaintiffs are at a substantial risk of identity theft or fraud." *McMorris*, 995 F.3d at 302 (emphasis added). Similar to the *McMorris* holding, the Court in *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) rejected the argument that "in order to establish standing, [p]laintiffs must allege . . . that they suffered some un-reimbursed or out of pocket expense.'"; *See*, *Rand v. Travelers' Indemnity Co*., 2022 WL 15523722 (S.D.N.Y. Oct. 27, 2022) ("Although plaintiff does not allege that her PII obtained from Traveler's agency portal, or that of other class members, was actually misused or that there was any attempted misuse after the data breach, 'misuse is not necessarily required.'" (quoting from *Clemens v. ExecuPharm Inc*., 48 F.4th 146, 154 (3d Cir. 2022)) *See also Remijas, supra* at 693 (noting that, consistent with the holding in *McMorris*, plaintiffs should not be required "to wait for the threatened harm to materialize in order to sue"); *Cotter v. Checkers Drive-In Restaurants, Inc*., 2021 WL 3773414 (M.D. Fla. August 25, 2021) (noting in a data breach case that the Eleventh Circuit has made clear that "evidence of actual identity theft or misuse is not

required to demonstrate standing"). The *Checkers* court noted that the Eleventh Circuit in *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 20921), a case Defendant relies on (Def. Mem. 17) "did not require that plaintiffs show 'some misuse' of their *own* data. Instead, the court required 'specific evidence of some misuse of *class members'* data.'" *Checkers*, at *5 (citing *Tsao* at 986 F.3d. 1344) (emphasis by the court); *See also, Miller v. Syracuse Univ.*, 2023 WL 2572937, at *11 (N.D.N.Y. March 20, 2023) (noting that, consistent with *McMorris*, "plaintiff has alleged at least one potential misuse of his data – ***the attempted*** bank fraud") (emphasis added).

With regard to current injury, "[a]ny monetary loss suffered by the plaintiff satisfies [the injury in fact] element; even a small; financial loss suffices.'" *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 55 (2d Cir. 2016).

Moreover, expenses reasonably incurred to mitigate the risk of identity theft in the future may also qualify as an injury-in-fact if the plaintiff plausibly alleges a substantial risk of the future identity theft. *Rand v. Travelers' Indemnity Co*., 2022 WL 15523722 (S.D.N.Y. Oct. 27, 2022); citing to *McMorris*, 995 F.3d at 303.

B. The Amended Complaint Alleges Present Injury or Substantial Risk of Future Injury

The landscape has changed tremendously since the filing of the initial complaint in this case. The effects of the Breach due to Ally's admitted negligence has spread like a mushroom cloud after an explosion, to the point Ally can no longer credibly claim that misuse to its account holders has not occurred. The evidence that it has is overwhelming.

The AC sets forth that on April 19, 2021, May 3, 2021 and August 11, 2021, Ally customers began reporting unauthorized thefts of their accounts demonstrating that within a mere weeks after the Breach was terminated, intrusions began occurring to putative class members resulting in monetary loss (AC ¶14). These documented incidents of misuse were well within the time period

cited by this Court as viable for traceability based on *Stollenwerk v. Tri-West Health Care Alliance*, 254 F.App'x 664, 667 (9th Cir. 2007). Individually, Plaintiff maintained a Coinbase account that was linked to his Ally Bank account. In October 2022, a fraudster used the Ally Bank password to improperly spend down the total value of cryptocurrency then on deposit on Plaintiff's Coinbase account and to also purchase $5,000 in Bitcoin in the account. This demonstrates malicious actors continued to have the ability to seek to cause Plaintiff financial losses which were actual and not merely theoretical. AC ¶¶109-112.

The AC also documents that because the Breach led to Ally freezing his account, he lost the ability to make securities trades that would have been profitable. While Defendant claims this claim is merely theoretical, the previous Declaration of David De Medicis, dated Nov. 24, 2021 (ECF No. 22)[2] makes clear that this is not the case, stating at ¶11:

> The problem was significant to me in part because I use this account from time to times to make securities trades. I learned of the lock out ***because I was attempting to deposit money into the account for the purposes of purchasing stocks and the timing was important for me.*** Unfortunately, because of the lock out, I could not transfer the funds and the stock purchases were no longer available at the prices I was intending to buy them at." (emphasis added)

This is clearly not aspirational but was actual, as was the loss. *See also*, AC ¶¶ 82-83, indicating Plaintiff intended to make these securities purchases in the Vanguard Russell 1000 Growth ETF.

In addition, the AC documents the explosion of account intrusions, hacked accounts, stolen funds and attempts to steal funds. AC ¶¶98-108. Examples include Ben Langhofer, who learned that his company received over 11,000 "test" transactions of $1 from Ally Bank Account holders' accounts, a typical method used by hackers to see if these minute transactions will go through

[2] Plaintiff incorporates the sworn de Medicis Declaration herein by reference.

before engaging in more robust fraud with the accounts. In addition, a tidal wave of online inquiries from Ally account holders about the fraud is documented on the AC. Traceability is not an issue with these incidents because they involve Ally accounts directly. In addition, these events directly contradict the Declaration of Christian Hall ("Hall Decl.") that Ally has not identified any increased rates of potential fraudulent activity (Hall Decl., ¶23). If the extreme number of fraudulent events documented online and sampled in the AC are normal for Ally, it is clear the company should be shut down immediately for its absence of security. Other than that vague statement in ¶23, the Hall Decl. is completely silent as to the rampant number of attacks described by Ally account holders and based on that, the Court should construe them as allegations of misuse directly traceable to the Ally Breach.[3] The Hall Decl. mentions the Plaintiff's Coinbase attack which is alleged to have been the result of that account being linked to his Ally account. But the Hall Decl. has no response to this other than to avoid it by stating "Ally has no control over or knowledge regarding Plaintiff's non-Ally accounts." Hall Decl., ¶32.

In sum, the current AC demonstrates sufficient misuse to give rise to standing derived from the current harm or future injury based on the continued and relentless attempts to misuse the Ally Data with regard to not only Plaintiff, but with regard to a large number of putative class members whose Ally accounts have been compromised.

As noted, "traceability" for Article III standing is a modest burden for plaintiff. *Toretto, supra*, at 472. Plaintiff's Amended Complaint satisfies that standard.

In addition, the tripartite test of *McMorris* is met here. *McMorris, Id.* at 303. *First*, the Plaintiff's data has been exposed as a result of an attack which, although initially the result of

[3] Indeed, one Ally account holder posts "Something is up with Ally – fraud tweets giant spike yesterday. Was there a data breach?" AC, ¶ 105-106.

Ally's admitted negligence, mushroomed into a serial hacking journey for Plaintiff and thousands of Ally customers who documented their losses online. *Second*, with regard to whether there has been misuse "even if plaintiffs themselves have not yet experienced identity theft or fraud" [*Id*. at 303] that is clearly satisfied based on the facts set forth in the AC outlining the myriad of intrusions to Ally account holders. The third element is whether the data that was exposed is sufficiently sensitive to create a risk of identity theft or fraud. While Ally argues account numbers are not, the facts here demonstrate that in the months-upon-months that Ally dawdled, the hackers who had gotten hold of the account numbers during the February to April 2021 time period, were able to get a running jump on exploiting the data, leading to the exponential fraud outlined in the AC, ¶¶ 14-16, 98-107 which the Hall Decl. is deafening silent on.

Moreover, limiting the time period as if this were the four quarters of a football game is unrealistic in the world of hacking. One example of this is described in the AC, ¶¶ 114-115. A hacker penetrated Plaintiff's Amazon account using the password Ally disseminated in the Breach. That hacker then attempted to make a purchase using Plaintiff's credit cards and bank account information that were obtained by his access to Plaintiff's Amazon account. Thus, one intrusion gives the key to unlock the next intrusion. This constitutes sufficient misuse and traceability to confer standing based on the high risk of future injury under *McMorris*. The Hall Declaration is silent on this intrusion, claiming total ignorance of the event. Hall Decl. ¶32.

Clearly, the AC demonstrates sufficient current injury in fact or substantial future risk of injury to confer standing on Plaintiff and the claims asserted herein.

III. THE COMPLAINT ADEQUATELY ALLEGES CLAIMS FOR RELIEF

A. Choice of Law

The Court must determine what law applies when considering a motion to dismiss. A federal court exercising diversity jurisdiction must apply the choice of law rules of the forum state

– here the State of New York. Under New York law, "the first step in any case presenting a potential choice of law issue is to determine whether there is an actual conflict between the laws of the jurisdictions involved." *Geron v. Seyfarth Shaw LLP (In re Thelen LLP)*, 736 F.3d 213, 219 (2d Cir. 2013). If there is conflict, New York requires that "the law of the jurisdiction having the greatest interest in the litigation will be applied . . ." *Id*.

New York distinguishes between torts involving conduct-regulating rules and loss-allocation rules in its interest-analysis. Because in this case "conduct-regulating laws are at issue, the law of the jurisdiction where the tort occurred will generally apply because that jurisdiction has the greatest interest in regulating behavior within its borders." *Cooney v. Osgood Mach., Inc*., 81 N.Y.2d 66, 72, 612 N.E.2d 277, 595 N.Y.S.2d 919 (1993). The alleged tort here involves the negligent programing, testing and monitoring of Ally's customer Website. Thus, New York, the jurisdiction where Ally negligently programmed, monitored and tested its customer Website has the greatest interest in regulating Ally's conduct. Similarly, for contract claims, New York "looks to the 'center of gravity' of a contract to determine choice of law." *AEI Life LLC v. Lincoln Ben. Life Co.*, 892 F.3d 126, 135 (2d Cir. 2018).

Without the benefit of discovery, however, Plaintiff is unable to determine with any degree of certainty where the alleged conduct occurred or where the "center of gravity" of the contract lies. Thus, any determinations of choice of law at this stage are premature.[4]

[4] Defendants' citation to *Schmitt v. SN Serv. Corp.*, 2021 WL 3493754, at *4 (N.D. Cal. Aug. 9, 2021) for the proposition that in data breach cases courts generally select the state where the company headquarters are located is true only so long as the negligent conduct occurred at the company headquarters. *Schmitt*, at *8. Unless Defendants are willing to concede that the negligent conduct emanated from the company headquarters in New York, further discovery is needed to engage in a more fulsome choice of law analysis.

B. Plaintiff Has Stated a Claim for Negligence

Under both Utah and Virginia law, "[t]o establish a claim of negligence, the plaintiff much establish four essential elements: (1) that the defendant owed the plaintiff a duty, (2) that the defendant breached that duty, (3) that the breach of duty was the proximate cause of the plaintiff's injury, and (4) that the plaintiff in fact suffered injuries or damages." *Gonzalez v. Russell Sorensen Const*., 279 P.3d 422, 428 (Court of Appeals Utah 2012); *see also Blue Ridge Service Corp. of Virginia v. Saxon Shoes, Inc.,* 271 Va. 206, 218 (S. Ct. Va. 2006). Regardless of which state law applies, Plaintiffs have adequately stated a claim for negligence.

1. Ally Owed Plaintiff a Duty of Care

Ally suggests it has no duty to Plaintiff, but this argument is without merit. Virginia courts have consistently reaffirmed that "[g]eneral negligence principles require a person to exercise due care to avoid injuring others" and that the "common law requires that every person must exercise ordinary care in the use and maintenance of his own property to prevent injury to others." *Quisenberry v. Huntington Ingalls Inc.,* 818 S.E.2d 805, 809-810 (Va. 2018) (internal quotation omitted) ("[W]henever one person is by circumstances placed in such a position with regard to another … that if he did not use ordinary care and skill in his own conduct with regard to those circumstances, he would cause danger of injury to the person or property of the other, a duty arises to use ordinary care and skill to avoid such injury.").

In fact, the decision in *In re Capital One Consumer Data Security Breach Litigation*, 488 F. Supp. 3d 374, 400-401 (E.D. Va. 2020), a case that Defendants rely on, found that plaintiff there had stated a claim for negligence in a data breach context. The facts in *Capital One* are substantially similar to the facts alleged by Plaintiff here. The present action and *Capital One* both involve customers that were required to provide their private information on an application as a pre-condition to becoming a customer and both companies continued to maintain that private

information and made representations to their customers that they would take the appropriate steps to ensure that their private information is protected and that they maintained adequate security measures. *Id.* at 399; AC ¶¶ 20-21.

Other courts applying these same general negligence principles—including courts in Utah—have held that companies who fail to exercise ordinary care with respect to their customers' sensitive information owe a duty of care in negligence. *See, e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig.,* 362 F. Supp. 3d 1295 at 1325 (N.D. Ga. 2019) ("*In re Equifax*") (holding Equifax "owed the Plaintiffs a duty of care to safeguard the personal information in its custody" that arose "from the allegations that [Equifax] knew a foreseeable risk to its data security systems but failed to implement reasonable security measures")[5].

The Complaint alleges that Defendants owed Plaintiff "a duty of care to use reasonable means to secure and safeguard" his private information that Ally collected as a condition for Plaintiff to open, use and maintain deposit and security accounts at Ally. In order to open up an account at Ally, Plaintiff had to create usernames and passwords and provide other non-public information. Ally owed Plaintiff a duty to implement proper procedures and practices to secure Plaintiff's private information.

Ally also assumed a duty to Plaintiff by voluntarily undertaking to maintain and store Plaintiff's private information and was required to do so with ordinary care. "'[O]ne who assumes

[5] *See also In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1309-10 (D. Minn. 2014) (finding plaintiffs "plausibly pled a general negligence case," at the motion to dismiss stage, where alleged Target "disable[ed] certain security features and fail[ed] to heed the warning signs of the hackers' attack began"); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *21 (D. Or. July 29, 2019) (stating that plaintiffs' negligence claim "with respect to Premera's provision of data security" was "relatively strong" where the insurer experienced a data breach affecting millions of customers and employees); *Brush v. Miami Beach Healthcare Grp. Ltd.,* 283 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) ("It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information").

to act, even though gratuitously, may thereby become subject to the duty of acting carefully, if he acts at all.' *Kellermann v. McDonough*, 278 Va. 478, 493-494, 684 S.E.2d 786, 791 (Va. 2009); *See also Nelson By and Through Stuckman v. Salt Lake City*, 919 P.2d 568, 573 (Utah 1996).

Ally actively solicited to store and maintain private information as part of its business and was solely responsible for ensuring its systems were sufficient to protect against the foreseeable risk of harm to those whose private information it maintained and stored. AC ¶¶ 19-21; 61-64. In undertaking to store and maintain Plaintiff's private information, Ally was aware of the risk of harm if it acted negligently, yet failed to implement adequate security measures which would have prevented the Breach. AC ¶¶ 2, 4-8, 19-24, 27-28, 37-42, 65-69.

The cases Defendants rely on are distinguishable. Ally argues that Virginia does not recognize a "common-law duty to protect electronic private information from unauthorized disclosure" and relies on two inapposite cases. The court in *Parker v. Carilion Clinic*, 819 S.E.2d 809, 823 (Va. 2018) dismissed the plaintiff's claim for tort liability against the employer because the employees did not act with the requisite corporate authority required for *respondent superior* liability, and therefore did not address whether a company can be directly liable for its own negligence under general negligence principles. The court also dismissed the plaintiff's negligence *per se* claim premised upon a violation of HIPAA but did not dismiss the claim because Virginia law does not recognize a common law duty to protect confidential information from disclosure or theft but because: "[n]one of our precedents has ever imposed a tort duty on a healthcare provider to manage its confidential information systems so as to deter employees from willfully gaining unauthorized access to confidential medical information." *Id*. at 825.[6]

[6]*Deutsche Bank Nat'l Trust Co. v. Buck*, 2019 WL 1440280, at *6 (E.D. Va. Mar. 29, 2019) is also distinguishable on its facts. There, Duetsche Bank engaged defendant Buck to perform a real estate transaction and engaged Altisource to act on its behalf and convey payment instructions to Buck. *Id*. at *1.

2. Plaintiff Alleges Damages

Defendants argue that Plaintiff's non-economic losses such as "increased risk of identity theft and time and effort to monitor accounts" are too speculative to support a negligence claim. However, Plaintiff's theory of damages is cognizable in the evolving context of data breach litigation. Here, Plaintiff has alleged economic damages (*e.g.*, failure to make securities trades and further injury), *as well as* non-economic damages including (a) paying monies to Ally for its goods and services which they would not have paid had Ally disclosed its inadequate data security practices; (b) damages to and diminution in the value of Plaintiff's private information—a form of intangible property that Plaintiff entrusted to Ally as a condition for opening Ally accounts; (c) loss of privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft. (AC ¶¶ 29, 33,47). *See, e.g.*, *In re Anthem, Inc. Data Breach Litigation.*, 162 F. Supp. 3d 953, 987 (N.D. Cal. 2016) at *12-16 ("[A] growing number of courts that have recognized that damages associated with time spent monitoring one's PII are recoverable.").[7] Plaintiff's alleged damages are cognizable in data breach cases and sufficient to survive a motion to dismiss.

C. Negligence *Per Se*

Both Utah and Virginia recognize negligence *per se* where a plaintiff alleges (1) "the defendant violated a statute enacted for public safety," (2) that he "belong[s] to the class of persons

---

A non-party hacker obtained information about the closing from Altisource tricking Buck to send the funds to the hacker. *Id.* at *2. Deutsche Bank sued the entity Altisource and the court acknowledged that "courts have found that a party may proceed on a negligence claim against an entity who suffered a data breach" but found that Buck, under the facts alleged, "fail[ed] to establish a legal duty *Altisource* owed to *Deutsche*[.]" *Id*. at *5.

[7] *See also Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) (holding "time and effort" plaintiff spent "monitoring both his card statements and his other financial information" was "sufficient" for standing); *In Re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197, 1224 (N.D. Ca. 2014) ("the risk that [p]laintiffs' personal data will be misused by the hackers who breached [defendant's] network is immediate and very real."); *In re Target Corporation Customer Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1166 (D. Minn. 2014) (accepting damages theory that plaintiffs "would not have shopped" had they known about the Target's data security issues).

for whose benefit the statute was enacted," (3) "that the harm that occurred was of the type against which the statute was designed to protect," and (4) "the statutory violation [was] a proximate cause of" his injury. *Collett v. Cordovana*, 290 Va. 139, 148, 772 S.E.2d 584, 589 (Va. 2015); *see also Rollins v. Petersen*, 813 P.2d 1156, 1163 (Utah 1991). While, as Defendants point out, the court in *In re Capital One*, 488 F. Supp. 3d at 408, dismissed plaintiffs' negligence *per se* claim based on a violation of the FTC Act, the court in *Bans Pasta, LLC, v. Mirko Franchising, LLC,* 2014 WL 637762, at *12 (W.D. Va. 2014) denied a motion to dismiss plaintiffs' negligence *per se* claim based on a violation of the FTC Franchise Rule (not a violation of Section 5 itself but promulgated under the FTC ACT) and stated that "[w]hile the Court understands Defendants' concern and shares it to some extent, both Georgia (and Virginia) law expressly allow negligence *per se* claims to be premised on statutes and regulations that do not give rise to a private cause of action." *Id*. at *12. Accordingly, Plaintiff's negligence *per se* claims premised upon a violation of the FTC Act can survive a motion to dismiss.

Further, Utah has allowed negligence *per se* to apply to federal statutes that do not provide a private right of action. *See Resolution Tr. Corp. v. Hess*, 820 F. Supp. 1359, 1368 (D. Utah 1993) ("the lack of a private right of action under [the federal Home Owners Loan Act] does not necessarily preclude the possibility of using [the Home Owners Loan Act] regulations as a standard of care in a federal common law claim for negligence *per se*"). For negligence *per se* to apply, the statute's purpose must be to protect a class of persons of which the plaintiffs are members and to protect against the type of harm experienced. *See Id*. at 1163-64, *Stembridge v. Nat'l Feeds, Inc.,* 2013 U.S. Dist. LEXIS 136789, *22-23 (D. UT. Sep. 23, 2013).

Here, Plaintiff's negligence *per se* claim arises from Ally's failure to comply with the FTC Act, which prohibits "unfair methods of competition in or affecting commerce." *See* 15 U.S.C. §

45 (a)(1). Under the FTC Act, the Federal Trade Commission ("FTC") has the authority "to declare unlawful an act or practice on the grounds that such an act of practice is unfair" if "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonable avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *See* 15 U.S.C. § 45 (n).

Several other district courts have recognized that a negligence *per se* claim can be based on a violation of the FTC Act in the data breach context. *Perdue v. Hy-Vee, Inc.,* No. 19-1330, 2020 WL 1917835, at *4 (C.D. Ill. Apr. 20, 2020) ("[C]ourts have held that the failure to maintain reasonable and appropriate data security for consumer's sensitive personal information can constitute an unfair method of competition in commerce in violation of the FTC. Therefore, the FTC Act can serve as the basis of a negligence *per se* claim."); *In re Equifax*, 362 F. Supp. 3d at 1327.[8]

Here, as in each of the cases cited above, Ally's failure to adopt and maintain reasonable security measures violates the FTC Act. *See* AC ¶¶ 72-76. Ally, as a merchant of commerce, is required to comply with the FTC Act's requirements, which are intended to protect customers, like Plaintiff and class members, from harm. *See* 15 U.S.C. § 45 (1) (prohibiting "unfair methods of competition in or affecting commerce"). The statute lays out the particular interests it seeks to

[8] *See also In re Arby's Restaurant Group Inc. Litig*., 2018 WL 2128441 at *8, (N.D. Ga. 2018); *In re The Home Depo, Inc. Customer Data Sec. Breach Litig.,* 2016 WL 2897520 at * 4 (N.D. Ga. 2016). Two circuit courts have expressly held that "unfair" or "deceptive" trade practices under Section 5 of the FTCA fairly encompass the failure to provide adequate data security measures to protect consumer financial data from threat of hacking. *See F.T.C. v. Wyndham Worldwide Corp.,* 799 F.3d 236, 247 (3d Cir. 2015) (affirming district court's denial of motion to dismiss claim brought by FTC against companies for alleged deficient cybersecurity that failed to protect customer data against hackers as unfair and deceptive practice in violation of § 5 of the FTCA); *In re TJX Companies Retail Sec. Breach Litig*., 564 F.3d 489, 498 (1st Cir. 2009) (denying motion to dismiss claim brought under Massachusetts statute prohibiting "unfair" or "deceptive" trade practices consistent with FTC's interpretation that defendant's lack of adequate security measures was unfair under the Federal Trade Commission Act).

protect: the privacy of customers, and protection of the security and confidentiality of the customer's nonpublic personal information. Plaintiff suffered the harm the statute was designed to protect against when Defendants failed to protect Plaintiff's private information.

D. Breach of Implied Contract

Both Virginia and Utah recognize that implied contracts are legal obligations created by words, actions, or circumstances. An implied contract is alleged with facts (1) showing mutual assent; (2) breach of the implied contract; and (3) damages. *Heidman v. Wash. City*, 155 P3d 900, 908 (Utah Ct. App. 2007); *Nossen v. Hoy*, 750 F. Supp. 740, 744 (E.D. Va. 1990). Whether an implied contract was formed is generally a question of fact and, thus, not appropriate for resolution on a motion to dismiss. *Hill v. Grand Cent., Inc.,* 25 Utah 2d 121, 477 P.2d 150 (1970).

The Amended Complaint alleges an implied contract formed by a course of conduct through which Ally solicited Plaintiff and the Class to provide Ally their private information as a precondition to Ally providing financial services. AC ¶ 79-80. *Spectra-4, LLP v. Uniwest Commercial Realty, Inc.*, 772 S.E.2d 290, 293 (Va. 2015). AC ¶ 81.

Courts routinely find that such allegations support a claim of implied contract in data breach litigation. *See e.g., Rudolph*, 2019 WL 2023713, at * 11 (collection cases); *Marriott*, 2020 WL 869241, at *29; *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 654, 675 (E.D. Pa. 2015), *aff'd sub nom*. *Enslin v. Coca-Cola Co.*, 739 F. App'x 91 (3d Cir. 2018) (concluding defendants, "through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard his PII").

"It is difficult to imagine how, in this day and age of data and identity theft, the mandatory receipt of . . . sensitive personal information would not imply the recipient's assent to protect the information sufficiently." *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at * 9 (N.D. Cal. Sept. 14, 2016). Ally promised Plaintiff and Class members that "***[Ally] will never share your***

username or password with anyone." AC ¶ 20. Ally further promised Plaintiff and Class members that Ally secured their private information with the latest encryption techniques.AC ¶ 21. Ally's promises could not have been more clear or explicit. Ally's argument that its policies were not sufficiently definite to be enforceable is wrong. Def. Mem. at 21. Courts construing corporate privacy notices in the data breach context frequently reject such arguments.[9] Ally admits that during "millions" of instances that customers used Ally's Website to access their Ally accounts, Ally wrongfully shared unencrypted usernames and passwords with third parties. Hall Decl., at ¶ 16.

Likewise, Plaintiff has plausibly alleged that Ally's statements are sufficiently definite promises of data security. Indeed, even Ally implicitly admitted it breached its implied contract with Plaintiff and the Class stating "we [Ally] know it's frustrating when our efforts don't live up to your expectations." Hall Decl., at Ex. A

Ally's disclosure of unencrypted usernames and passwords damaged the Plaintiff and Class. Securing private information is a fundamental element of providing financial services.

Ally wrongfully contends that Plaintiff has not stated compensable contract damages. Ally's breach of the implied contract deprived Plaintiff and Class members of the benefit-of-the-bargain. *See Alexander v. Brown*, 646 P.2d 692, 695 (Utah Sup. Ct. 1982) (breach of contract damages are properly measured by the amount necessary to place the nonbreaching party in as

[9] For example, In *Fero v. Excellus Heath Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017), on reconsideration *sub nom*. *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018) the court found the following promises sufficiently define to create an enforceable promise of data security: (1) "We are committed to safeguarding your protected health information"; (2) We "will not give out your nonpublic personal information to anyone unless we are permitted to do so by law." (3) "It is our policy to keep all information about you confidential in all settings." (4) "[W]e have a security coordinator to detect and prevent security breaches."; and (5) "[A]ll computer systems that contain personal information have security protections." *Id*.

good a position as if the contract had been performed); The post-trial cases Ally relies upon are not applicable.[10]

Ally's argument that Plaintiff's other injuries including actual and risk of future identity theft, costs to mitigate these harms, and loss of value of private information also fail because these types of harms arise from and are a foreseeable consequence of Ally's Breach. Ally knew these types of harms that would be imposed on Plaintiff if Ally failed to secure his username and password. *See*, *Richmond Med. Supply Co. v. Clifton*, 369 S.E.2d 407, 409 (1988).

E. Virginia Personal Information Breach Notification Act

Virginia Personal Information Breach Notification Act ("VPIBNA") requires that a company that experiences a data breach must give notice to "any resident of the Commonwealth" whose "personal information" is compromised. Va. Code § 18.2-186.6(B). Ally notified the Plaintiff by letter that his data was compromised. AC ¶ 1, Hall Decl. at Ex. A.

Ally's contention that the security breach did not reveal "personal information" within the meaning of the VPIBNA is misplaced. *First*, the Breach revealed unencrypted usernames and passwords. AC ¶¶ 2, 4, 22. *Second*, the very purpose of Ally usernames and passwords is to access, and *link* to, the Plaintiff's and Class member's unencrypted private information such as their first and last names and financial account numbers. AC ¶¶ 4-5, 22, 27-28. Va. Code § 18.2-186.6(A). Ally ignores that the Breach exposed more than usernames and passwords.

Plaintiff alleges all violations constituting a breach under the VPIBNA. Va. Code § 18.2-186.6(A). The Amended Complaint alleges a "breach of the security of the [Ally] system". AC ¶¶

[10] *See Shively v. Utah Valley Univ.*, No. 2:20-cv-119, 2020 U.S. Dist. LEXIS 129534, at *8 (D. Utah July 20, 2020) (a professor claiming breach of implied contract for wrongful suspension was not harmed because the suspension was *with pay*).

1-10, 19-29. Va. Code § 18.2-186.6(A). Ally's request that third parties delete certain files evidences the unauthorized acquisition of unencrypted and unredacted usernames and passwords. AC ¶ 23; Hall Decl. ¶ 18. The Breach compromised the security of personal information of multiple individuals – here "millions" of customer logins. AC ¶¶ 1, 53; Hall Decl. ¶ 16. Finally, that Ally reasonably believed the Breach "has caused, or will cause, identity theft or other fraud" is evidenced by, among other things, Ally's immediate commencement of "fraud monitoring efforts" to affected Ally accounts. Hall Decl. ¶ 15, and Ex. A. The Complaint alleges the Breach has caused, or will reasonably cause, Plaintiff to suffer identity theft. AC ¶¶ 30-35, 50-51. Finally, the VPIBNA applies to *all* unauthorized access that compromises the security and confidentiality of personal information, not just malicious hacking.

Ally violated the VPIBNA by failing to notify Plaintiff and Class members for two months after Ally discovered the Breach. Despite fully knowing when, where and how the security of its system was breached and the need for immediate commencement of fraud monitoring efforts, Ally's self-serving two-month lag in issuing its Breach notice was unreasonable. Va. Code § 18.2-186.6(B). Ally could have published a general notice of the Breach on April 12, 2021. Parsing through millions of logins before notifying the public merely provided a time lag for Ally to formulate a strategy to downplay its massive Breach. AC ¶¶ 8, 22. Nonetheless, the timeliness of the notice is a fact question not ripe for a motion to dismiss. *In re Capital One.*, 488 F. Supp. 3d at 416.

Finally, the Amended Complaint alleges Plaintiff suffered economic damages. Va. Code § 18.2-186.6(I). As in *In Re Capital One*, the Plaintiff here alleges identity theft, and is distinguishable from the plaintiff in *Corona v. Sony Pictures,* 2015 WL 3916744. *See In Re Capital One,* 488 F. Supp. 3d at 430. In the Complaint, Plaintiff asserts damages specific to the

failure of Ally Bank's notification of the Breach. Plaintiff suffered actual injury including diminution in value of his private information, lost time, annoyance, interference, and inconvenience. AC ¶¶ 33, 35.

F. **Plaintiff States a Claim under the NCUDTPA**

The elements of a NCUDTPA claim are that (i) an unfair or deceptive practice; (ii) in or affecting commerce; and (iii) that caused plaintiff's injury. *Country Club of Johnston Cty., Inc. v. United States Fid. & Guar. Co.*, 150 N.C. App. 231, 245, 563 S.E.2d 269, 278-79 (2002). NCUDTPA is remedial and claims thereunder are "construed liberally…" *Hicks v. Albertson*, 284 N.C. 236, 239, 200 S.E.2d 40 (1973). The statute is intended to "encourage private enforcement of NCUDTPA violations." *Marshall v. Miller*, 302 N.C. 539, 546, 276 S.E.2d 397, 401 (1981).

A practice is deceptive if it "possesse[s] the tendency or capacity to mislead, or create[s] the likelihood of deception." *Overstreet v. Brookland, Inc.*, 52 N.C. App. 444, 453, 279 S.E.2d 1, 7 (1981). Plaintiff alleges several statements made through Ally.com were misleading and omitted material facts. Such as "[W]e never share your usernames and passwords with anyone" and "For your protection, only people who need your information to do their jobs have access to the personal information you provide us . . ." possessed the capacity to mislead because they misrepresented and omitted facts about the true level of data security at Ally Bank and omitted that Ally.com was, in fact, compromising Sign-in Credentials and Private Information.[11] Plaintiff need not show fraud, bad faith, or intentional misrepresentation. *Melton v. Family First*

[11]In *Manos v. Freedom Mortg. Corp.*, No. 21-1324, 2022 U.S. App. LEXIS 7833, at *5 (4th Cir. Mar. 24, 2022), cited by Defendants, the court dismissed a NCUDTPA claim on summary judgment given undisputed evidence of constructive and actual disclosure of the alleged omitted facts. The opposite of the facts in the instant action.

Mortg. Corp., 156 N.C. App. 129, 576 S.E.2d 365 (2003).[12] Unauthorized disclosure compromising the confidentiality of Plaintiff's bank Sign-In Credentials violated established public policy.

Misleading statements were made via Ally.com. Ally.com was operated from Charlotte, North Carolina. Where an out of state plaintiff's injury resulted from alleged misrepresentations made by defendant, "in all probability, in North Carolina," the court denied defendant's motion to dismiss the out of state plaintiff's NCUDTPA claim. *Hardee's Food Sys. v. Beardmore*, No. 5:96-CV-508-BR(2), 1997 U.S. Dist. LEXIS 9671, at *10 (E.D.N.C. June 6, 1997).

Defendants' deceptive and unfair conduct affected commerce in North Carolina. *Hajmm Co. v. House of Raeford Farms, Inc.*, 328 N.C. 578, 592-93, 403 S.E.2d 483, 492 (1991) (commerce includes all business activities with few exceptions not applicable here).

Plaintiff pleads that Ally stored his Sign-in Credentials and Private Information at Ally's facility in North Carolina and therefore wrongfully disseminated from North Carolina. [13]

The AC alleges that the personnel responsible for Ally.com and the computer systems used to store Sign-In Credentials and Private Information are in Ally's Corporate Center in Charlotte, North Carolina. AC 31-33. Ally's unfair and deceptive conduct involves misleading statements, reckless or negligent data security practices, unauthorized dissemination of Sign-In

[12] *Edwards v. Genex Coop., Inc.*, 777 F. App'x 613, 624 (4th Cir. 2019) is distinguishable. There the plaintiff pled only a breach of contract claim which was dismissed on summary judgment. The plaintiff in *Edwards* was not granted leave to amend to allege a NCUDTPA claim based on the dismissed breach of contract claim.

[13] *The 'In' Porters, S.A. v. Hanes Printables, Inc.*, 663 F. Supp. 494, 495 (M.D.N.C. 1987) dismissed on jurisdictional grounds is inapplicable. In *Porters*, the record showed exclusively foreign misconduct with damages exclusively to foreign operations. In this action, misrepresentations made, in all probability, from North Carolina, caused injury so there is no inquiry into the sufficiency of Plaintiff's relationship to North Carolina as in *Porters*. North Carolina's long-arm statute explicitly confers jurisdiction "[i]n any action claiming injury to person or property [] within or without this State arising out of an act or omission within this State by the defendant." Section 1-75.4(3), *Verona v. U.S. Bancorp*, No. 7:09-CV-057-BR, 2011 U.S. Dist. LEXIS 33160, at *43 (E.D.N.C. Mar. 29, 2011).

Credentials for a period spanning three months, unreasonably delaying disclosure of the Breach, and then disclosing the Breach in a misleading manner so to minimize Ally's wrongful conduct. Such conduct caused injuries to the Plaintiff as set forth above.

G. Plaintiff States a Claim for Injunctive/Declaratory Relief

The Plaintiff is entitled to injunctive or declaratory relief under the Declaration Judgement Act, 28 U.S.C. § 2201. Despite Ally's contention otherwise, the Amended Complaint sufficiently alleges underlying violations and therefore states a valid legal predicate for injunctive or declaratory relief.

The Amended Complaint pleads woefully inadequate data security practices at Ally that persisted for months. Ally has not disclosed how the so called Coding Error manifested, nor steps taken to prevent a similar breach from occurring again, or how the Breach was allowed to persist for months purportedly undetected at Ally. The Amended Complaint sufficiently alleges Plaintiff and the Class are likely to suffer future injury from similar conduct. *Deshawn E. by Charlotte E. v. Safir*, 156 F.3d 340, 344 (2d Cir. 1998).

Conclusion

For all the foregoing reasons, the Court should deny Defendants' motion in its entirely.

Dated: April 5, 2023

Gary S. Graifman, Esq.
Melissa R. Emert, Esq.
KANTROWITZ GOLDHAMER & GRAIFMAN. P.C.
747 Chestnut Ridge Road, Suite 200
Chestnut Ridge, NY 10977
memert@kgglaw.com
ggraifman@gmail.com
T: (845) 356-2570

Patrick Slyne, Esq.
SLYNE LAW LLC
800 Westchester Avenue, N641
Rye Brook, NY 10573
patrick.slyne@slynelaw.com
T: (914) 279-7000
F: (914) 653-8122

Jonathan Shub, Esq.
SHUB LAW FIRM LLC
134 Kings Highway East, 2nd Floor
Haddonfield, NJ 08033
jshub@shublawyers.com
T: (856) 772-7200

Attorneys for the Plaintiff and Members of the Putative Class